Enclosure 2:

NASA Agency Selection and Tailoring of NIST 800-53 Security Controls: Moderate

Revision A
FINAL
Last Revised: 10/12/2006

Introduction:

The following security controls from the National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems,* are selected and tailored per NIST SP 800-53 tailoring procedures as NASA Agency Common Controls. As per Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information,* and the NASA Senior Agency Information Security Officer (SAISO) Memorandum "Agency Selection and Tailoring of Information Technology Security Controls"*,* these controls are mandatory for all NASA systems categorized as MODERATE. These controls are required to be addressed for the Certification and Accreditation of all MODERATE NASA Master and Subordinate System Security Plans (SSPs).

The IT Security Standard Operating Procedures (ITS-SOPs) referenced in this document are mandatory for use once they are published on the NASA Online Directives Information System (NODIS).

Each Center CIOs will issue and maintain an authoritative memorandum on Site Controls applicable to their Center, and possibly to specific sites within their Center. Any necessary Site Controls identified in the Agency Controls will be defined in these Site Control memoranda.

Format of each Control

Each control is described in the same NASA-defined format, as shown in Figure 1. Each section of the control description is explained in Figure 2.

[Control #] [Control Name]

This control is:
[ ] Agency Defined (see Control or NASA Control Enhancement)
[ ] Implemented and Verified by the Agency - no system owner action required (see Implementation Detail)
[ ] Selected for Annual Review by Agency

[ ] Master Plan Defined (see Control or NASA Control Enhancement)
[ ] Implemented and Verified by the Master system - no Subordinate system owner action required (see Implementation Detail)
[ ] Selected for Annual Review by Master Plan

[ ] Site Defined
[ ] Implemented and Verified by the Site - no system owner action required (see Implementation Detail)
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation Detail)
[ ] Selected for Annual Review by System Owner

[ ] Not Applicable to this System (see Implementation Detail for justification)
[ ] Not Accepted (see Implementation Detail for justification)

Control:

Supplemental Guidance:

NASA Control Enhancement:

Implementation Detail:

Figure 1. NASA-defined format for description of IT security controls

[Control #] [Control Name]

This control is:
[ ] Agency Defined (see Control or NASA Control Enhancement)
A check in this box indicates that this control is tailored at the Agency level and all systems, Master and Subordinate, must meet the requirements if the control is accepted. Master and Subordinate plans may not uncheck this box.
[ ] Implemented and Verified by the Agency - no system owner action required (see Implementation Detail)
A check in this box indicates that the control is implemented by the Agency and has been verified as meeting the NIST SP 800-53 requirements. No tailoring is necessary by Master security plans, and no additional implementation detail is required.
[ ] Selected for Annual Review by Agency
A check in this box indicates that the control will be reviewed annually during the continuous monitoring between C&As. This review can be part of the annual self-assessment by the system owner and shall include verifying that the control is still applicable, reasonable, effective and functioning as intended.

[ ] Master Plan Defined (see Control or NASA Control Enhancement)
A check in this box indicates that this control is tailored by the Master plan and the requirements must be met by all Subordinate systems under the Master's purview. The Master plan should provide details of the tailoring in the Control or NASA Control Enhancement section.
[ ] Implemented and Verified by the Master system - no Subordinate system owner action required (see Implementation Detail)
A check in this box indicates that the control is implemented by the Master plan and has been verified as meeting the NIST SP 800-53 requirements.
[ ] Selected for Annual Review by Master Plan
A check in this box indicates that the control will be reviewed annually during the continuous monitoring between C&As.

[ ] Site Defined
A check in this box indicates that this control is tailored by the Site.
[ ] Implemented and Verified by the Site - no system owner action required (see Implementation Detail)
A check in this box indicates that the control is implemented by the Site and has been verified as meeting the NIST 800-53 requirements. Processes and procedures are currently being established.
[ ] Selected for Annual Review by Site.
A check in this box indicates that the control will be reviewed annually during the continuous monitoring between C&As.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation Detail)
This indicates that the control is implemented by the Subordinate system and the implementation is described in the Implementation Detail.

[ ] Selected for Annual Review by System Owner

A check in this box indicates that the control will be reviewed annually during the continuous monitoring between C&As.

[ ] Not Applicable to this System (see Implementation Detail for justification)

A check in this box indicates that the control is deemed "not applicable" to the plan, Master or Subordinate. Justification must be provided in the Implementation Detail section and approved by the Master system's AO.

[ ] Not Accepted (see Implementation Detail for justification)

This indicates that the control is not implemented on the system, for example due to cost constraints or because it is not necessary to adequately protect the system. Justification must be provided in the Implementation Detail section and approved by the system's AO.

Control:

This is the control description from NIST SP 800-53. If the NIST 800-53 control has "organization defined parameters," such parameters are defined by Agency, Master Plan, or Site and specified in the Control section.

Supplemental Guidance:

If applicable, this is the description from NIST SP 800-53.

NASA Control Enhancement:

Description of any NASA-specific control tailoring or enhancements by Agency, Master Plan or Site. Additional tailoring guidance is given in ITS-SOP-0011 for Master controls.

Implementation Detail:

Description of implementation by Agency, Master Plan, Site or Subordinate Plan; OR reference to POA&M for actions to be completed; OR justification for Not Applicable; OR justification for Not Accepted

Figure 2. Explanation of NASA-defined format for IT security controls

Controls

13.1 MANAGEMENT CONTROLS

13.1.1 Risk Assessment (RA)

RA-1 Risk Assessment Policy and Procedures

This control is:

[ ] Agency Defined (see Control or NASA Control Enhancement).

[X] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).

[ ] Selected for Annual Review by System Owner.

[ ] Not Applicable to this plan (see Implementation Detail for justification).

[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:

The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

NASA Control Enhancement:

Implementation Detail:

Item (i) Control satisfied via NPR 2810.1A, *Security of Information Technology*, Section 12.2 - Risk Management Process Requirements and NPR 1620.2, *Physical Security Vulnerability Risk Assessments*. Item (ii) Control satisfied via NPR 2810.1A, *Security of Information Technology,* Section 12.2 – Risk Management Process Requirements and ITS-SOP-0019B, *Procedure for the FIPS-199 Categorization of Information Systems.*

RA-2 Security Categorization

This control is:

[X] Agency Defined (see Control or NASA Control Enhancement)

[ ] Implemented and Verified by the Agency - no system owner action required (see Implementation Detail)

[ ] Selected for Annual Review by Agency

[ ] Master Plan Defined (see Control or NASA Control Enhancement)

[ ] Implemented and Verified by the Master system - no Subordinate system owner action required (see Implementation Detail)

[ ] Selected for Annual Review by Master Plan

[ ] Site Defined

[ ] Implemented and Verified by the Site - no system owner action required (see Implementation Detail)

[ ] Selected for Annual Review by Site

[ ] Implemented and Verified by Subordinate System Owner (see Implementation Detail)

[ ] Selected for Annual Review by System Owner

[ ] Not Applicable to this System (see Implementation Detail for justification)

[ ] Not Accepted (see Implementation Detail for justification)

Control:
The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with FIPS 199 and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations.

NASA Control Enhancement:
NASA ITS-SOP-0019B shall be utilized for all information system security categorizations. The Master Security Plan, if present, shall set the FIPS-199 Impact Level and the Subordinate Security Plan is aligned to the appropriate Master Plan with the same Impact Level as the Subordinate.

Implementation Detail:

RA-3 Risk Assessment

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement)
[ ] Implemented and Verified by the Agency - no system owner action required (see Implementation Detail)
    [ ] Selected for Annual Review by Agency

[ ] Master Plan Defined (see Control or NASA Control Enhancement)
[ ] Implemented and Verified by the Master system - no Subordinate system owner action required (see Implementation Detail)
    [ ] Selected for Annual Review by Master Plan

[ ] Site Defined
[ ] Implemented and Verified by the Site - no system owner action required (see Implementation Detail)
    [ ] Selected for Annual Review by Site

[ ] Implemented and Verified by Subordinate System Owner (see Implementation Detail)
    [ ] Selected for Annual Review by System Owner

[ ] Not Applicable to this System (see Implementation Detail for justification)
[ ] Not Accepted (see Implementation Detail for justification)

Control:
The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.

NASA Control Enhancement:
Information system Risk Assessments are performed as part of the security planning process. Risk Assessments are summarized in the System Security Plan (SSP) and attached as an appendix to the SSP.

Implementation Detail:

RA-4 Risk Assessment Update

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement)
[ ] Implemented and Verified by the Agency - no system owner action required (see Implementation Detail)
[ ] Selected for Annual Review by Agency

[ ] Master Plan Defined (see Control or NASA Control Enhancement)
[ ] Implemented and Verified by the Master system - no Subordinate system owner action required (see Implementation Detail)
[ ] Selected for Annual Review by Master Plan

[ ] Site Defined
[ ] Implemented and Verified by the Site - no system owner action required (see Implementation Detail)
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation Detail)
[ ] Selected for Annual Review by System Owner

[ ] Not Applicable to this System (see Implementation Detail for justification)
[ ] Not Accepted (see Implementation Detail for justification)

Control:
The organization updates the risk assessment {**per continuous monitoring requirements defined in NASA Certification and Accreditation phase 4**} or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.

NASA Control Enhancement:
The system owner utilizes the Agency Security Plan and Documentation System to update and store the information system Risk Assessment.
The Center ITSMs review information system Risk Assessments under their purview prior to submission to the Authorizing Official (AO) and take appropriate to action to ensure that a Risk Assessment is completed for each SSP and that it addresses all Federal and NASA security requirements.

Implementation Detail:

RA-5 Vulnerability Scanning

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
Using appropriate vulnerability scanning tools and techniques, the organization scans for vulnerabilities in the information system {**quarterly, at a minimum**} or when significant new vulnerabilities affecting the system are identified and reported.

(1) Vulnerability scanning tools include the capability to readily update the list of vulnerabilities scanned.
(2) The organization updates the list of information system vulnerabilities {quarterly, at a minimum} or when significant new vulnerabilities are identified and reported.

NASA Control Enhancement:
Agency Top 30 vulnerability assessment scans are performed on a quarterly basis (specifically the 1st of March, June, September & December), in accordance with the NASA CIO Letter on *Scanning and Vulnerability Elimination or Mitigation*, dated December 19, 2003. Quarterly vulnerability scan reports are submitted to NASIRC at the end of each quarter.

Implementation Detail:

13.1.2 Planning (PL)

PL-1 Security Planning Policy and Procedures

This control is:
[ ] Agency Defined (see Control or NASA Control Enhancement).
[X] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
 [ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
 [ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
 [ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
 [ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.

NASA Control Enhancement:

Implementation Detail:
Item (i) Control satisfied via NPR 2810.1A, *Security of Information Technology*, Chapter 13 - IT System Security Planning. Item (ii) Control satisfied via NASA ITS-SOP-0011, *Procedure for Development and Life-Cycle of NASA Master Security Plans* (when finalized); ITS-SOP-0016, *Subordinate IT Security Plan Template Requirements, Guidance, and Examples;* ITS-SOP-0032, *Master IT Security Plan Template Requirements, Guidance, and Examples,* ITS-SOP-0018, *Contractor ITS Program Plan Procedure,* NASA ITS-SOP-0030, *Certification and Accreditation of FIPS-199 High and Moderate Systems*; and ITS-SOP-0031, *Certification and Accreditation of FIPS-199 Low Systems*, ITS-SOP-0019B, *Procedure for the FIPS-199 Categorization of Information*

Systems, and ITS-SOP-0007, *NASA Master and Subordinate System Security Plan Numbering Schema.*

PL-2 System Security Plan

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).

Control:
The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.

NASA Control Enhancement:
System Security Plan requirements are defined in Chapter 13 of NPR 2810.1A, *Security of Information Technology*. The System Security Plan template for Subordinate systems is defined in NASA ITS-SOP-0016. The security plans template for Master systems is defined in ITS-SOP-0032. As per OCIO Memorandum "ITSM Responsibilities with Respect to Agency and Program Systems", April 14, 2006, the Center ITSM ensures that all information systems under their purview are associated with an up-to-date system security plan.

Implementation Detail:

PL-3 System Security Plan Update

This control is:

[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization reviews the security plan for the information system {every three (3) years} and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.

NASA Control Enhancement:
NASA SSPs shall be reviewed at a minimum of every three years via the NASA Certification and Accreditation process defined in NASA ITS-SOP-0030, *Certification and Accreditation of FIPS-199 High and Moderate Systems*; and ITS-SOP-0031, *Certification and Accreditation of FIPS-199 Low Systems*.

Implementation Detail:

PL-5 Privacy Impact Assessment

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ]	Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
	[ ]	Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
	[ ]	Selected for Annual Review by System Owner.
[ ]	Not Applicable to this plan (see Implementation Detail for justification).
[ ]	Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization conducts a privacy impact assessment on the information system.

NASA Control Enhancement:
NASA systems shall perform a Privacy Impact Assessment (PIA) in accordance with the Agency Privacy Office instructions. All systems shall ensure that Personally Identifiable Information (PII) is identified in accordance with OMB Memorandum M-06-16, *Protection of Sensitive Agency Information,* June, 23, 2006.

Implementation Detail:

13.1.3 System and Services Acquisition (SA)

SA-1 System and Services Acquisition Policy and Procedures

This control is:
[ ]	Agency Defined (see Control or NASA Control Enhancement).
[X] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
	[ ]	Selected for Annual Review by Agency.

[ ]	Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
	[ ]	Selected for Annual Review by Master.

[ ]	Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
	[ ]	Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).

[ ] Selected for Annual Review by System Owner.

[ ] Not Applicable to this plan (see Implementation Detail for justification).

[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

NASA Control Enhancement:

Implementation Detail:
Item (i) Control satisfied via NPR 2810.1A, *Security of Information Technology*, Chapter 10 – "Products and Services" Sections 10.1-10.4. Item (ii) Control satisfied via NASA FAR Supplement 1852.204-76 and NASA contract IT Security Clause.

SA-6 Software Usage Restrictions

This control is:

[X] Agency Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).

[ ] Selected for Annual Review by System Owner.

[ ] Not Applicable to this plan (see Implementation Detail for justification).

[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization complies with software usage restrictions.

NASA Control Enhancement:
An annual review of the software within the information system is conducted to ensure that usage restrictions as defined in NPR 2810.1 are being complied with. To the extent possible, the organization employs tracking systems to control copying and distribution of software.

Implementation Detail:

SA-8 Security Design Principles

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization designs and implements the information system using security engineering principles.

NASA Control Enhancement:
The principles defined in NIST SP 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, Revision A, shall be utilized by Master and Subordinate Systems throughout the System Development Lifecycle (SDLC) to address this control. The Master Security Plan and Subordinate Security plans shall provide appropriate detail for tracing the principles from 800-27 to the SDLC.

Implementation Detail

SA-9 Outsourced Information System Services

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization ensures that third-party providers of information system services employ adequate security controls in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements. The organization monitors security control compliance.

NASA Control Enhancement:
The NASA IT Security Clause shall be included in all NASA contracts, in accordance with NASA procurement office instructions and the Federal Acquisition Regulation (FAR).

The Center ITSM with IT security responsibility over each non-NASA system containing NASA data that is critical to NASA's mission or operation, and over each contractor or external NASA system or facility ensures that the security controls of the system or facility are assessed annually using ITS-SOP-005B, *Completing a NASA IT Security Program or System Assessment*. The Center ITSM reports security control compliance to the Senior Agency Information Security Officer (SAISO) quarterly for Center and Agency systems under their purview.

Implementation Detail:

13.1.4 Certification, Accreditation, and Security Assessments (CA)

CA-1 Certification, Accreditation, and Security Assessments

This control is:
[ ] Agency Defined (see Control or NASA Control Enhancement).
[X] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.

NASA Control Enhancement:

Implementation Detail:
Item (i) Control satisfied via NPR 2810.1A, *Security of Information Technology*, Chapter 14 – Certification and Accreditation. Item (ii) Control satisfied via procedures found in NASA ITS-SOP-0030, *Certification and Accreditation of FIPS-199 High and Moderate Systems*; ITS-SOP-0031, *Certification and Accreditation of FIPS-199 Low Systems*; ITS-SOP-006, *Procedure for Extending an IT System Authorization to Operate*; and ITS-SOP-005B, *Completing a NASA IT Security Program or System Assessment*.

CA-3 Information Systems Connections

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
    [ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization authorizes {and documents} all connections from the information system to other information systems outside of the accreditation boundary and monitors/controls the system interconnections on an ongoing basis. Appropriate organizational officials approve information system interconnection agreements.

NASA Control Enhancements:
All authorizations are documented in accordance with ITS-SOP-0041, *Procedure for IT Systems Interconnections,* (when finalized).

Implementation Detail:

CA-4 Security Certification

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).

[ ] Selected for Annual Review by System Owner.

[ ] Not Applicable to this plan (see Implementation Detail for justification).

[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

NASA Control Enhancements:
NASA ITS-SOP-0030, *NASA IT System Certification and Accreditation of FIPS-199 High and Moderate Systems,* shall be utilized for the security certification process of High and Moderate category information systems while ITS-SOP-0031, *NASA IT System Certification and Accreditation of FIPS-199 Low Systems,* shall be utilized for the security certification process of Low category information systems.

Implementation Detail:

13.2 OPERATIONAL CONTROLS

13.2.1 Personnel Security (PS)

PS-1 Personnel Security Policy and Procedures

This control is:

[ ] Agency Defined (see Control or NASA Control Enhancement).

[X] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).

[ ] Selected for Annual Review by System Owner.

[ ] Not Applicable to this plan (see Implementation Detail for justification).

[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

NASA Control Enhancement:

Implementation Detail:
Item (i) and (ii) Control satisfied via NPR 1600.1, *NASA Security Program Procedural Requirements,* Chapters 1, 2, 3, 4 and 7.

PS-2 Position Categorization

This control is:

[X] Agency Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).

[ ] Selected for Annual Review by System Owner.

[ ] Not Applicable to this plan (see Implementation Detail for justification).

[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations {at least annually as part of System Review}.

NASA Control Enhancement:
Control implementation requirements are detailed in NPR 1600.1, *NASA Security Program Procedural Requirements,* Chapters 2,3 and 4 and are consistent with Office of Personnel Management (OPM) 5 CF 731.106(a).

Implementation Detail:

PS-3 Personnel Screening

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization screens individuals requiring access to organizational information and information systems before authorizing access.

NASA Control Enhancement:
Control implementation requirements are detailed in NPR 1600.1, *NASA Security Program Procedural Requirements,* Chapters 2, 3 and 4.

Implementation Detail:

PS-7 Third-Party Personnel Security

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
    [ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization establishes personnel security requirements for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management) and monitors provider compliance to ensure adequate security.

NASA Control Enhancement:
Control implementation requirements are detailed in NPR 1600.1, *NASA Security Program Procedural Requirements,* Chapters 2, 3 and 4

Implementation Detail:

PS-8 Personnel Sanctions

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
    [ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

NASA Control Enhancement:
Control implementation requirements are detailed in NPR 1600.1, *NASA Security Program Procedural Requirements,* Section 1.4 “Violations of Security Requirements”.

Implementation Detail:

13.2.2 Physical and Environmental Protection (PE)

PE-1 Physical and Environmental Protection Policy and Procedures

This control is:
[ ] Agency Defined (see Control or NASA Control Enhancement).
[X] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).

[ ] Selected for Annual Review by System Owner.

[ ] Not Applicable to this plan (see Implementation Detail for justification).

[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

NASA Control Enhancement:

Implementation Detail:
Item (i) Control satisfied via NPR 2810.1A, *Security of Information Technology,* Chapter 14 Section IV "Operational Controls" and NPR 1600.1, *NASA Security Program Procedural Requirements*. Item (ii) Control satisfied via NPR 8831.2D Chapter 3 "Facilities Maintenance Management".

13.2.3 Contingency Planning (CP)

CP-1 Contingency Planning Policy and Procedures

This control is:

[ ] Agency Defined (see Control or NASA Control Enhancement).

[X] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).

[ ] Selected for Annual Review by System Owner.

[ ] Not Applicable to this plan (see Implementation Detail for justification).

[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

NASA Control Enhancement:

Implementation Detail:
Item (i) Control satisfied via NPR 2810.1A, *Security of Information Technology,* Chapter 15 "System Contingency Planning". Item (ii) Control satisfied via NPR 1040.1, *Continuity of Operations Planning (COOP) Procedures and Guidelines* and by ITS-SOP-0040, *Procedures for Contingency Planning* (when finalized).

13.2.4 Configuration Management (CM)

CM-1 Configuration Management Policy and Procedures

This control is:

[ ] Agency Defined (see Control or NASA Control Enhancement).

[X] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).

[ ] Selected for Annual Review by System Owner.

[ ] Not Applicable to this plan (see Implementation Detail for justification).

[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

NASA Control Enhancement:

Implementation Detail:
Item (i) Control satisfied via NPR 2810.1A, *Security of Information Technology,* Section 16.5 – Configuration Management. Item (ii) Control satisfied by ITS-SOP-0014, *Procedure for Approving Changes to NASA's Information Technology Baseline.*

CM-6 Configuration Settings

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
    [ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization configures the security settings of information technology products to the most restrictive mode consistent with information system operational requirements.

(1) The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.

NASA Control Enhancement:
Detailed settings requirements are provided by OCIO Memos on the Implementation of Center for Internet Security (CIS) Benchmarks dated 9/2/04 & 6/29/05.
Additional detail is provided by OCIO Memo "FY 2006 Patch Management and Security Configuration Metrics", dated 3/9/06 which establishes the Agency Security Configuration Standards (ASCS) project (http://desktop-standards.nasa.gov/CIS/).

Implementation Detail:

13.2.5 Maintenance (MA)

MA-1 System Maintenance Policy and Procedures

This control is:
[ ] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[X] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.

NASA Control Enhancements:

Implementation Detail:
Item (i) Control satisfied via NPR 2810.1A, *Security of Information Technology,* Section 16.5 – Configuration Management. Item (ii) Control satisfied by ITS-SOP-0039, *Procedure for IT System Maintenance Controls* (when finalized).

13.2.6 System and Information Integrity (SI)

SI-1 System and Information Integrity Policy and Procedures

This control is:
[ ] Agency Defined (see Control or NASA Control Enhancement).
[X] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

NASA Control Enhancement:

Implementation Detail:
Item (i) Control satisfied via NPR 2810.1A, *Security of Information Technology,* sections 2.2.3.1, 2.3.3.1, 2.3.6.2, 2.4.7.2, 11.3.8.3, 11.3.10.2, 16.5.4.1, 16.5.4.2.1, & 17.1.3
Item (ii) Control satisfied via NASA ITS-SOP-0005B, *Completing a NASA IT Security Program or System Assessment;* ITS-SOP-0008, *Procedure for Initiating and Managing*

Targeted Monitoring of Electronic Data; ITS-SOP-0013, *Procedure for Routine NASA Network and Context Monitoring;* ITS-SOP-0014, *Procedure for Approving Changes to NASA's Information Technology Baseline;* ITS-SOP-0017, *It Security Penetration Test Plan and Rules of Engagement;* ITS-SOP-0021, *Network Security Vulnerability Scanning;* ITS-SOP-0030, *IT System Certification and Accreditation Process for Moderate and High Systems;* ITS-SOP-0031, *IT System Certification and Accreditation Process for Low Systems*.

SI-2 Flaw Remediation

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
    [ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization identifies, reports, and corrects information system flaws.

NASA Control Enhancement:
Information system flaws are identified, reported and corrected in accordance with the NASA CIO Letter on *Scanning and Vulnerability Elimination or Mitigation*, dated December 19, 2003. Security patches are applied based on their identified criticality to the information system following the procedures identified in ITS-SOP-0012, *NASA Patch Selection and Reporting Procedure*. Each Center shall maintain a Site Control for SI-2 that defines requirements automatic updates and central management.

Implementation Detail:

SI-3 Malicious Code Protection

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
  [ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
  [ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
  [ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
  [ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The information system implements malicious code protection that includes a capability for automatic updates.

(1) The organization centrally manages virus protection mechanisms.
(2) The information system automatically updates virus protection mechanisms.

NASA Control Enhancement:
Antivirus software shall be installed on all NASA systems. The Center shall maintain a Site Control for SI-3 that defines the requirements at Center-level for the central management of virus protection and automatic updates.

Implementation Detail:

SI-4 Intrusion Detection Tools and Techniques

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
  [ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
    [ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.

NASA Control Enhancement:
Monitoring shall be achieved via a combination of Network Intrusion Detection System (IDS), Host IDS (servers, critical workstations), log monitoring and network forensic tools. To the extent possible, automated tools are utilized for Intrusion Detection and log analysis. Techniques for targeted monitoring are defined in ITS-SOP-0008, *Procedure for Initiating and Managing Targeted Monitoring of electronic Data.*

Implementation Detail:

SI-5 Security Alerts and Advisories

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[X] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).

[ ] Selected for Annual Review by System Owner.

[ ] Not Applicable to this plan (see Implementation Detail for justification).

[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.

NASA Control Enhancement:
In addition to implementation at the Agency level, each NASA system shall follow the NASIRC security alert procedures ITS-SOP-0015, *Procedures for Agency IT Security Incident Classification and Reporting* and track advisories and alerts according to system impact.

Implementation Detail:
The NASA Incident Response Center (NASIRC) receives and disseminates information system security alerts/advisories from government and industry sources and issues NASA-specific alerts and advisories to the NASA IT community. NASIRC disseminates a consolidated security advisory daily to Center's and appropriate NASA IT Security personnel.

13.2.7 Media Protection (MP)

MP-1 Media Protection Policy and Procedures

This control is:

[ ] Agency Defined (see Control or NASA Control Enhancement).

[X] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).

[ ] Selected for Annual Review by System Owner.

[ ] Not Applicable to this plan (see Implementation Detail for justification).

[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:

The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.

NASA Control Enhancement:

Implementation Detail:

Item (i) Control satisfied by NPR 1600.1 and NPR 1620. Item (ii) Control satisfied by ITS-SOP-0033, *Procedure for the Protection of Electronic Media.*

MP-3 Media Labeling

This control is:

[X] Agency Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).

[ ] Selected for Annual Review by System Owner.

[ ] Not Applicable to this plan (see Implementation Detail for justification).

[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:

The organization affixes external labels to removable information storage media and information system output indicating the distribution limitations and handling caveats of the information. The organization exempts the following specific types of media or hardware components from labeling so long as they remain within a secure environment: {***as per NPR 1600.1, NPR 1620, and ITS-SOP-0034, Procedure for the Labeling of Electronic Media***}.

NASA Control Enhancement:
All systems handling NASA information shall use ITS-SOP-0034 (when finalized) for the appropriate labeling of electronic media.

Implementation Detail:

MP-6 Media Sanitization

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization sanitizes information system digital media using approved equipment, techniques, and procedures. The organization tracks, documents, and verifies media sanitization actions and periodically tests sanitization equipment/procedures to ensure correct performance.

NASA Control Enhancement:
NASA ITS-SOP-0035, *Procedure for the Sanitation of Electronic Media* (when finalized), addresses Media Sanitization for NASA IT systems and shall be utilized by System Owners to properly track, document, and verify media sanitization on their

systems.

Implementation Detail:

MP-7 Media Destruction and Disposal

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization sanitizes or destroys information system digital media before its disposal or release for reuse outside the organization, to prevent unauthorized individuals from gaining access to and using the information contained on the media.

NASA Control Enhancement:
NASA ITS-SOP-0035, *Procedure for the Sanitization of Electronic Media* (when finalized), addresses Media Sanitization, Destruction, and Disposal procedures as defined by OCIO and OSPP. All systems carrying NASA information shall incorporate ITS-SOP-0035 into the sanitization, destruction, and disposal of NASA information contained in electronic media.

Implementation Detail:

13.2.8 Incident Response (IR)

IR-1 Incident Response Policy and Procedures

This control is:
[ ] Agency Defined (see Control or NASA Control Enhancement).
[X] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

NASA Control Enhancement:

Implementation Detail:
Item (i) Control satisfied by NPR 2810.1A, *Security of Information Technology,* Chapter 17 and OCIO Memo "Information Technology Security (ITS) Incident Reporting Requirements" dated 6/29/03, 8/29/03, 12/4/04. Item (ii) Control satisfied by ITS-SOP-0015, *Incident Classification Reporting* and ITS-SOP-0012, *Determining Cost Impact of IT Security Incidents.* NASA's incident response policy and procedures are based on guidance provided by NIST publications SP 800-61 "Computer Security Incident Handling Guide", SP800-83 "Guide to Malware Incident Prevention and Handling", SP800-86 "Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response".

IR-2 Incident Response Training

This control is:

[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training {**annually**}.

NASA Control Enhancement:
the System for Administration, Training, and Educational Resources (SATERN) shall maintain all NASA Agency IT Security training documentation and modules for compliance, including defining incident response roles and responsibilities.

Implementation Detail:

IR-4 Incident Handling

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).

    [ ]	Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).

    [ ]	Selected for Annual Review by System Owner.

[ ]	Not Applicable to this plan (see Implementation Detail for justification).

[ ]	Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization implements an incident handling capability for security incidents that includes preparation, detection, analysis, containment, eradication, and recovery.

(1) The organization employs automated mechanisms to support the incident handling process.

NASA Control Enhancement:
NASA ITS-SOP-015, *Agency IT Security Incident Classification Reporting,* and ITS-SOP-0022, define procedures for incident handling. The SOP's are based on guidance provided by NIST publications SP 800-61, *Computer Security Incident Handling Guide*; SP 800-83, *Guide to Malware Incident Prevention and Handling*, SP 800-86, *Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response*, and shall be utilized across the agency to ensure common methods of data collection and analysis.

Implementation Detail:

IR-5 Incident Monitoring

This control is:

[X]	Agency Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).

    [ ]	Selected for Annual Review by Agency.

[ ]	Master Plan Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).

    [ ]	Selected for Annual Review by Master.

[ ]	Site Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).

    [ ]	Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).

[ ] Selected for Annual Review by System Owner.

[ ] Not Applicable to this plan (see Implementation Detail for justification).

[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization tracks and documents information system security incidents on an ongoing basis.

NASA Control Enhancement:
NASA ITS-SOP-0015, *Procedures for Agency IT Security Incident Classification and Reporting* shall be used to classify and report incidents in coordination with OSPP and OIG. NIST SP800-61, *Computer Security Incident Handling Guide* shall be used for guidance in defining procedures and methods.

Implementation Detail:

IR-6 Incident Reporting

This control is:

[X] Agency Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).

[ ] Selected for Annual Review by System Owner.

[ ] Not Applicable to this plan (see Implementation Detail for justification).

[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization promptly reports incident information to appropriate authorities. Supplemental Guidance: The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consistent with applicable federal laws, directives, policies, regulations, standards,

and guidance.

(1) The organization employs automated mechanisms to assist in the reporting of security incidents.

NASA Control Enhancement:
NPR 2810.1A, *Security of Information Technology,* Chapter 17 and ITS-SOP-0015, *Agency IT Security Incident Classification Reporting* define the NASA incident reporting requirements.

Implementation Detail:

IR-7 Incident Response Assistance

This control is:
[ ] Agency Defined (see Control or NASA Control Enhancement).
[X] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization provides an incident support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability.

(1) The organization employs automated mechanisms to increase the availability of incident response-related information and support.

NASA Control Enhancement:

Implementation Detail:
Incident response assistance shall be provided through the NASA Incident Response Center (NASIRC) at http://www-nasirc.nasa.gov/.

13.2.9 Awareness and Training (AT)

AT-1 Security Awareness and Training Policy and Procedures

This control is:
[ ] Agency Defined (see Control or NASA Control Enhancement).
[X] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
    [ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

NASA Control Enhancement:

Implementation Detail:
Item (i) Control satisfied via NPR 2810.1A, *Security of Information Technology*, Chapter 18 – IT Security Awareness and Training. Item (ii) Control satisfied via procedures found in OCIO Directive Letter regarding IT Security Awareness and Training annual metrics and in the NASA OCIO Directive Letter; Subject: "IT Security Certification for

Computer and Network Administrators”; dated November 25, 2002.

AT-2 Security Awareness

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization ensures all users (including managers and senior executives) are exposed to basic information system security awareness materials before authorizing access to the system and {**annually**} thereafter.

NASA Control Enhancement:
Control adherence is achieved via the System for Administration, Training, and Educational Resources (SATERN) Basic IT Security and IT Security for Managers, both of which are updated annually, as well as center specific annual security reviews. System access authorization based on security awareness training is a manual process.

Implementation Detail:

AT-3 Security Training

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization identifies personnel with significant information system security roles and responsibilities, documents those roles and responsibilities, and provides appropriate information system security training before authorizing access to the system and every three years thereafter.

NASA Control Enhancement:
Key management, system administrators, and network administrators are required to obtain annual training as defined by the SAISO. NASA OCIO Directive, Subject: "IT Security Certification for Computer and Network Administrators", dated November 25, 2002, requires all networked computer systems and devices to have an assigned System Administrator responsible for IT Security with a NASA 3rd Party in-house certification (in good standing). Center CIO's are responsible to ensure that system administrators at their Center have received certification from a professionally recognized organization.

Implementation Detail:

AT-4 Security Training Records

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.

NASA Control Enhancement:
NASA IT Security Training reporting requirements are defined in the NASA CIO Letter on *F&04 Reporting Requirements for Information Technology Security Training*, dated December 19, 2003. SATERN is the central repository of NASA Agency IT Security training documentation.

Implementation Detail:

13.3 TECHNICAL CONTROLS

13.3.1 Identification and Authentication (IA)

IA-1 Identification and Authentication Policy and Procedures

This control is:
[ ] Agency Defined (see Control or NASA Control Enhancement).
[X] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

NASA Control Enhancement:

Implementation Detail:
Item (i) Control satisfied via NPR 2810.1A, *Security of Information Technology,* Section 19.1 - Identification and Authentication. (ii) Control satisfied via ITS-SOP-0036, *NASA Common Identification and Authentication Procedures* (when finalized).

13.3.2 Access Control (AC)

AC-1 Access Control Policy and Procedures

This control is:
[ ] Agency Defined (see Control or NASA Control Enhancement).
[X] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.

[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

NASA Control Enhancement:

Implementation Detail:
Item (i) Control satisfied via NPR 2810.1A, *Security of Information Technology*, Chapter 19 – Identification and Authentication, and Chapter 20 – Logical Access Controls.
Item(ii) defined by ITS-SOP-0037, *NASA Common Access Controls Procedures for IT Systems* (when finalized).

AC-8 System Use Notification

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to

criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

NASA Control Enhancement:
The NASA approved warning banner shall be displayed on all NASA computers and applications in accordance with NPR 2810.1A, Section 11.3.6.

Implementation Detail:

AC-18 Wireless Access Restrictions

This control is:
[ ] Agency Defined (see Control or NASA Control Enhancement).
[X] [**Partially**] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) documents, monitors, and controls wireless access to the information system. Appropriate organizational officials authorize the use of wireless technologies.

(1) The organization uses authentication and encryption to protect wireless access to the information system.

NASA Control Enhancement:
Item (ii) Control to be satisfied by system owners.

Implementation Detail:
Item (i) Control satisfied via NPR 2810.1A, *Security of Information Technology*, Section 11.3.10 – Use of Wireless Local Area Networks and via NASA ITS-SOP-0020, *Wireless Local Area Network Implementation*. Additional guidance on wireless security is provided by NIST SP 800-48, *Wireless Network Security 802.11, Bluetooth, and Handheld Devices*.

AC-20 Personally Owned Information Systems

This control is:
[ ] Agency Defined (see Control or NASA Control Enhancement).
[X] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization restricts the use of personally owned information systems for official U.S. Government business involving the processing, storage, or transmission of federal information.

NASA Control Enhancement:
NPR 2810.1A, *Security of Information Technology*, Section 11.3.5. "Personal-Owned and Company IT Resources." and NPD 2540.1, *Personal Use of Government Office Equipment Including Information Technology,* provide the requirements and guidance for personally owned information systems.

Implementation Detail:

13.3.3 Audit and Accountability (AU)

AU-1 Audit and Accountability Policy and Procedures

This control is:
[ ] Agency Defined (see Control or NASA Control Enhancement).
[X] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

NASA Control Enhancement:

Implementation Detail:
Item (i) Control satisfied via NPR 2810.1A, *Security of Information Technology*, Chapter 21 - Audit Trails and Accountability. Item (ii) Control satisfied via ITS-SOP-0038, *Procedures for Auditing and Accountability Controls* (when finalized).

AU-2 Auditable Events

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).

[ ] Selected for Annual Review by System Owner.

[ ] Not Applicable to this plan (see Implementation Detail for justification).

[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:

NASA information systems generate audit records, at a minimum, for the following events. The events labeled Personally Identifiable Information (PII) and International Traffic in Arms Regulations (ITAR):

Minimum events to be audited

Startup and shutdown
Authentication
Authorization/permission granting
Action by trusted users
Process invocation
Unsuccessful data access attempt (threshold=log on five unsuccessful attempts)
Data deletion (PII/ITAR)
Data transfer (PII/ITAR)
Application configuration change
Application of confidentiality or integrity labels to data (PII/ITAR)
Override or modification of data labels or markings (PII/ITAR)
Output to removable media (PII/ITAR)
Output to a printer (PII/ITAR)

Event items required to be associated with each audited event

UserID/ProcessID causing the event
Event Success/Failure
Event Date/Time (GMT)
Type of Event
Source IP Address

NASA Control Enhancement:

Implementation Detail:

AU-3 Content of Audit Records

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The information system captures sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events.

(1) The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.

NASA Control Enhancement:
NASA systems shall implement the audit log minimum requirements as per Security Control AU-2.

Implementation Detail:

AU-8 Time Stamps

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
[ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The information system provides time stamps for use in audit record generation.

NASA Control Enhancement:
NASA time stamps are synchronized to one or more of the NIST time servers.

Implementation Detail:

AU-9 Protection of Audit Information

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).

[ ] Selected for Annual Review by System Owner.

[ ] Not Applicable to this plan (see Implementation Detail for justification).

[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

NASA Control Enhancement:
As per Deputy Administrator Memorandum, July 26, 2006, "Meeting NASA Minimum IT Security Requirements", NASA information systems shall implement the principle of least privilege for all audit information and tools.

Implementation Detail:

AU-11 Audit Retention

This control is:

[X] Agency Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).

[ ] Selected for Annual Review by System Owner.

[ ] Not Applicable to this plan (see Implementation Detail for justification).

[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization retains audit logs for {**minimum of one years**} to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

NASA Control Enhancement:

Audit record retention policies and procedures are defined in NPR 1441.1D, *NASA Records and Retention Schedules* and as per Deputy Administrator Memorandum, July 26, 2006, “Meeting NASA Minimum IT Security Requirements”, all audit records shall be stored for a minimum for one year.

Implementation Detail:

13.3.4 System and Communications Protection (SC)

SC-1 System and Communications Protection Policy and Procedures

This control is:
[ ]   Agency Defined (see Control or NASA Control Enhancement).
[X] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
    [ ]   Selected for Annual Review by Agency.

[ ]   Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
    [ ]   Selected for Annual Review by Master.

[ ]   Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
    [ ]   Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
    [ ]   Selected for Annual Review by System Owner.
[ ]   Not Applicable to this plan (see Implementation Detail for justification).
[ ]   Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

NASA Control Enhancement:

Implementation Detail:
Item (i) Control satisfied via NPR 2810.1A, *Security of Information Technology*, Section 11.3.14 – System and Communication Protection Requirements. Item (ii) Control

satisfied via ITS-SOP-0039, *Procedure for System and Communications Protection Controls* (when finalized).

SC-17 Public Key Infrastructure Certificates

This control is:
[ ] Agency Defined (see Control or NASA Control Enhancement).
[X] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
    [ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization develops and implements a certificate policy and certification practice statement for the issuance of public key certificates used in the information system.

NASA Control Enhancement:

Implementation Detail:
Control satisfied via X.509 *Certificate Policy for National Aeronautics and Space Administration (NASA) Public Key Infrastructure (PKI),* December 17, 2004, Revision 1.3.1.2; and *NASA Certification Authority Certification Practice Statement*, December 17, 2004, Revision 1.3.1.2.

SC-18 Mobile Code

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[X] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
    [ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
  [ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).
  [ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).
  [ ] Selected for Annual Review by System Owner.
[ ] Not Applicable to this plan (see Implementation Detail for justification).
[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) documents, monitors, and controls the use of mobile code within the information system. Appropriate organizational officials authorize the use of mobile code.

NASA Control Enhancement:
Item (ii) Control to be satisfied by system owners.

Implementation Detail:
Item (i) Control: NIST Special Publications SP 800-28, *Guidelines on Active Content and Mobile Code* and SP 800-19, *Mobile Agent Security* shall be utilized as guidance for this control.

SC-19 Voice Over Internet Protocol

This control is:
[X] Agency Defined (see Control or NASA Control Enhancement).
[X] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).
  [ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).
[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).
  [ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).

[ ] Selected for Annual Review by System Owner.

[ ] Not Applicable to this plan (see Implementation Detail for justification).

[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control:
The organization: (i) establishes usage restrictions and implementation guidance for Voice Over Internet Protocol (VOIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) documents, monitors, and controls the use of VOIP within the information system. Appropriate organizational officials authorize the use of VOIP.

NASA Control Enhancement:
Item (ii) Control to be satisfied by system owners.

Implementation Detail:
Item (i) Control: NIST SP 800-58, *Security Considerations for Voice Over IP (VOIP) Systems* shall be utilized for guidance on VOIP security & implementation.

13.4 NASA SPECIFIC CONTROLS

NASA Controls are NASA unique requirements that are not mapped to a specific NIST SP 800-53 Control. NASA controls are to be address by all system owners regardless of the high water mark.

13.4.1 NASA National Security Criticality

This control is:

[X] Agency Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Agency - no System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Agency.

[ ] Master Plan Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Master - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Master.

[ ] Site Defined (see Control or NASA Control Enhancement).

[ ] Implemented and Verified by Site - no Subordinate System Owner action required (see Implementation detail).

[ ] Selected for Annual Review by Site.

[ ] Implemented and Verified by Subordinate System Owner (see Implementation detail).

[ ] Selected for Annual Review by System Owner.

[ ] Not Applicable to this plan (see Implementation Detail for justification).

[ ] Not Accepted by System Owner (see Implementation Detail for justification).

Control: Mission Essential Infrastructure (MEI) Systems are identified by NASA and reported to the Department of Homeland Security (DHS) for registry.

NASA Control Enhancement:

Implementation Detail: